F3 Éléments de correction

Ex 1

$S_1 : \begin{cases} x \equiv 2 \ [7] \\ x \equiv 3 \ [11] \end{cases}$ admet des solutions car $pgcd(7,11) = 1$.

Une relation de Bezout entre 11 et 7 est obtenue à partir de l'algorithme d'Euclide : $11 = 7 + 4$, $7 = 4 + 3$, $4 = 3 + 1$ donc

$1 = 4 - 3 = 4 - (7 - 4) = 2 \times 4 - 7 = 2(11 - 7) - 7 = 2 \times 11 - 3 \times 7 = 7u + 11v$

avec $u = -3$, $v = 2$. Or $\begin{cases} 7u \equiv 0 \ [7] \\ 7u \equiv 1 \ [11] \end{cases}$ $\begin{cases} 11v \equiv 1 \ [7] \\ 11v \equiv 0 \ [11] \end{cases}$ donc

$x_0 = 2 \times 11v + 3 \times 7u = 44 - 63 = -19$ est solution particulière de S_1

La solution générale s'obtient en écrivant $S_1 \Leftrightarrow \begin{cases} x \equiv x_0 \ [7] \\ x \equiv x_0 \ [11] \end{cases} \Leftrightarrow$

$\begin{cases} 7 \mid x - x_0 \\ 11 \mid x - x_0 \end{cases} \Leftrightarrow \underset{ppcm(7,11)}{\underset{\shortparallel}{77}} \mid x - x_0 \Leftrightarrow x \equiv x_0 \ [77] \Leftrightarrow x \equiv -19 \ [77] \Leftrightarrow x \equiv 58 \ [77]$

$S_2 : \begin{cases} x \equiv 4 \ [21] \\ x \equiv 10 \ [33] \end{cases} \Rightarrow \begin{cases} x \equiv 4 \ [3] \\ x \equiv 10 \ [3] \end{cases}$ (où $3 = pgcd(21,33)$) $\Rightarrow 4 \equiv 10 \ [3]$ ce qui est vrai, donc S_2 admet des solutions.

On les trouve en passant à $S_2' : \begin{cases} x \equiv 4 \ [7] \\ x \equiv 10 \ [11] \end{cases}$ où la relation de Bezout

ci-dessus $7u + 11v = 1$ avec $u = -3$, $v = 2$ peut être de nouveau utilisée.

On a cette fois-ci $x_0 = 10 \cdot 7u + 4 \times 11v = -210 + 88 = -122$ solution particulière de S_2', mais aussi de S_2. Alors $S_2 \Leftrightarrow \begin{cases} x \equiv x_0 \ [21] \\ x \equiv x_0 \ [33] \end{cases} \Leftrightarrow$

$\begin{cases} 21 \mid x - x_0 \\ 33 \mid x - x_0 \end{cases} \Leftrightarrow ppcm(21,33) = 231 \mid x - x_0 \Leftrightarrow x \equiv x_0 \ [231] \Leftrightarrow x \equiv -122 \ [231]$

$\Leftrightarrow x \equiv 109 \ [231]$.

Enfin $S_3 \begin{cases} x \equiv 3 \ [17] \\ x \equiv 4 \ [11] \\ x \equiv 5 \ [6] \end{cases}$ se résoud par étapes : on s'occupe d'abord de

$S_3^1 : \begin{cases} x \equiv 3 \ [17] \\ x \equiv 4 \ [11] \end{cases}$ avec $pgcd(17,11) = 1$

On a F3 ©

$17 = 11 + 6$, $11 = 6+5$, $6 = 5+1$ d'où $1 = 6-5$, $1 = 6 - (11-6) =$

$= 2\times 6 - 11 = 2(17-11) - 11 = 2\times 17 - 3\times 11$. Alors $x_0 = 4\times 2\times 17 - 3\times 5\times 11 = 37$ est solution particulière de S_3^1 et la solution générale s'obtient à partir de

$$\begin{cases} x \equiv x_0 \ [17] \\ x \equiv x_0 \ [11] \end{cases} \iff x \equiv x_0 \ [187] \quad \text{avec } 187 = \text{ppcm}(17,11)$$

Alors $S_3 \iff \begin{cases} x \equiv 37 \ [187] \\ x \equiv 5 \ [6] \end{cases}$ avec $\text{pgcd}(187,6) = 1$. On a

$187 = 6\times 31 + 1$ donc $1 = 187 - 31\times 6$ et une solution particulière

$x_0 = 5\times 187 - 37\times 31\times 6 = -5947$. Donc $S_3 \iff \begin{cases} x \equiv x_0 \ [187] \\ x \equiv x_0 \ [6] \end{cases}$

$\iff x \equiv x_0 \ [1122]$ car $1122 = \text{ppcm}(187,6) \iff x \equiv -5947 \ [1122]$

$\iff x \equiv 785 \ [1122]$.

Ex 2 La loi n'est pas commutative car la table n'est pas symétrique par rapport à la première diagonale : on a par exemple $xy = t$ et $yx = z \neq t$.

La loi n'est pas associative car $(xy)z = tz = x$ et $x(yz) = xt = z \neq x$. Donc ce n'est pas une loi de groupe.

D'ailleurs, d'après l'exercice 5, si cette table était la table d'un groupe G, comme G vérifie les conditions de l'exercice 5. D'après cet exercice G devrait alors être commutatif, ce qui n'est pas le cas.

Ex 3 La loi d'un groupe d'ordre 2 ne peut être que

$*$	e	x
e	e	x
x	x	e

car $e*e = e$, $e*x = x$, $x*e = x$ et $x*x = e$ (non que $x*x = x$ donnerait $x = e$)

En général pour un groupe G l'application "translation" par $g \in G$

$t_g : G \longrightarrow G$, $x \longmapsto gx$ est une bijection de G dans G (d'inverse $t_{g^{-1}}$

$t_{g^{-1}} : G \longrightarrow G$, $x \longmapsto g^{-1}x$) donc toutes les

lignes d'une table de groupe comportent que des éléments distincts (la ligne correspondant à g est formée par $gx_1, gx_2, \ldots, gx_n$ si $G = \{x_1, \ldots, x_n\}$ et $gx_i \neq gx_j$ $\forall i \neq j$)

De même toutes les colonnes d'une table de groupe comportent que des éléments distincts car la colonne correspondant à g est formée par $x_1 g, x_2 g, \ldots, x_n g$ si $G = \{x_1, \ldots, x_n\}$ et $x_i g \neq x_j g$ $\forall i \neq j$ (si $x_i g = x_j g$ alors $x_i \underbrace{g g^{-1}}_{e} = x_j \underbrace{g g^{-1}}_{e}$ donc $x_i = x_j$ donc $i = j$).

Les tables des groupes ressemblent donc à des "sudokus", sans que cette propriété soit suffisante pour qu'une table la vérifiant soit la table d'un groupe. En effet, la table de l'ex 2 respecte cette règle des "sudokus" car il n'y a aucune répétition ni en ligne, ni en colonne. Et pourtant ce n'est pas la table d'un groupe.

Revenons à l'unique table possible pour un groupe à deux éléments. L'existence de l'élément neutre et des inverses sont assurées par la construction même de la table ($x^{-1} = x$) et pour vérifier qu'il s'agit bien d'un groupe il reste à vérifier l'associativité de $*$.

Pour nous épargner cela, nous allons considérer un groupe connu à 2 éléments, comme $(\mathbb{Z}/2\mathbb{Z}, +)$ ou $(U_2, \cdot) = (\{\pm 1\}, \cdot)$. Comme leurs tables sont

$\mathbb{Z}/2\mathbb{Z}$

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

U_2

$\cdot$	1	-1
1	1	-1
-1	-1	1

cela signifie bien que G

$*$	e	x
e	e	x
x	x	e

est la table d'un groupe (unique possibilité donc pour un groupe à 2 éléments)

En effet dans le modèle $G=\mathbb{Z}/2\mathbb{Z}$, $*=+$, $e=\bar{0}$, $x=\bar{1}$ les tables coïncident et pareil pour $G=\mathbb{U}_2$, $*=\cdot$, $e=1$, $x=-1$.
On aurait pu aussi vérifier l'associativité directement car en présence de deux éléments seulement il n'y a pas beaucoup de cas à considérer mais cette vérification devient fastidieuse dès que l'on passe à des groupes de 3 ou 4 éléments. Notre connaissance de groupes à 3 ou 4 éléments permettra de se convaincre plus vite que certaines tables représentent des opérations associatives.

Ex4 On essaye, comme à l'exercice précédent, de construire des tables pour $G=\{e,x,y\}$ et $G=\{e,x,y,z\}$ en respectant les propriétés de l'élément neutre et des "sudokus" (c.à.d pas de répétition dans les lignes et les colonnes). Quand la complétion de la table comporte un choix, on entourera cet élément et on donnera les autres choix faits par la suite. Quand il n'y a pas de choix possible on n'entourera pas les éléments considérés.

G

$\cdot$	e	x	y
e	e	x	y
x	x	e	y
y	y		

répétition

choix impossible

donc la seule table possible est

$\cdot$	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

Dans cette table il reste à vérifier l'associativité.

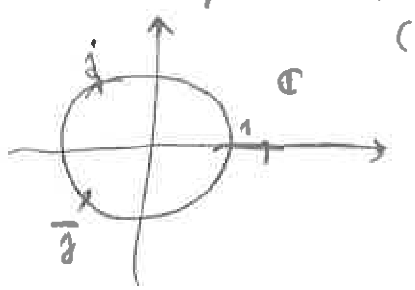
Pour éviter trop de calculs considérons plutôt la table de $(\mathbb{Z}/3\mathbb{Z},+)$ et montrons que pour $e=\bar{0}$, $x=\bar{1}$, $y=\bar{2}$ il s'agit de la même table.

En effet $\mathbb{Z}/3\mathbb{Z}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Il y a donc une seule structure de groupe possible sur un ensemble à 3 éléments. La table sera la même pour $G=\mathbb{U}_3$, $e=1$, $x=e^{\frac{2i\pi}{3}}=j$, $y=e^{-\frac{2i\pi}{3}}=\bar{j}$ $(j^3=1)$

$\mathbb{U}_3 \cdot$	1	j	$\bar{j}=j^2$
1	1	j	$\bar{j}$
j	j	$\bar{j}$	1
$\bar{j}$	$\bar{j}$	1	j



On a représenté $\mathbb{U}_3=\{1,j,\bar{j}\}$ dans le plan complexe $\mathbb{C}$.

Si $G = \{e, x, y, z\}$ on a

G_1

$\cdot$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

ou (variation du premier choix dans G_1)

G_2

$\cdot$	e	x	y	z
e	e	x	y	z
x	x	y	z	e
y	y	z	e	x
z	z	e	x	y

en fait ce n'est pas vraiment un choix car prendre x à cette place produit une répétition dans la dernière colonne

ou

G_3

$\cdot$	e	x	y	z
e	e	x	y	z
x	x	z	e	y
y	y	e	z	x
z	z	y	x	e

pas le choix ici, sinon répétition dans la dernière colonne

Il reste à varier le second choix de G_1

G_4

$\cdot$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	x	e
z	z	y	e	x

Nous voici en présence de 4 tables possibles, pour lesquelles il faudrait vérifier l'associativité, considérons à cet effet la table du groupe connu $(\mathbb{Z}/4\mathbb{Z}, +)$

$\mathbb{Z}/4\mathbb{Z}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Pour $e = \bar{0}$, $x = \bar{1}$, $y = \bar{2}$, $z = \bar{3}$ c'est exactement G_2, donc $(G_2, \cdot)$ est la table d'un groupe de même structure que $(\mathbb{Z}/4\mathbb{Z}, +)$.

Pour $e = \bar{0}$, $x = \bar{2}$, $y = \bar{1}$, $z = \bar{3}$ c'est la table G_4 donc $(G_4, \cdot)$ est aussi la table d'un groupe de même structure que $(\mathbb{Z}/4\mathbb{Z}, +)$

Pour $e = \bar{0}$, $x = \bar{3}$, $y = \bar{1}$, $z = \bar{2}$ c'est la table G_3 donc $(G_3, \cdot)$ est la table d'un groupe de même structure que $(\mathbb{Z}/4\mathbb{Z}, +)$ aussi.

Considérons maintenant l'ensemble $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(x_1,x_2) \mid x_1,x_2 \in \mathbb{Z}/2\mathbb{Z}\}$ avec la loi $(x_1,x_2)+(y_1,y_2) = (x_1+y_1, x_2+y_2)$ les additions se faisant composante par composante comme dans $\mathbb{Z}/2\mathbb{Z}$. On appelle ce groupe le groupe produit de $G_1 = (\mathbb{Z}/2\mathbb{Z},+)$ et de $G_2 = (\mathbb{Z}/2\mathbb{Z},+)$.

Un tel produit de groupes est en général de nouveau un groupe G noté $G_1 \times G_2 = \{(g_1,g_2) \mid g_1 \in G_1, g_2 \in G_2\}$ pour la loi

$(g_1,g_2) * (h_1,h_2) = (g_1h_1, g_2h_2)$ les compositions des éléments se faisant composante par composante en utilisant les lois correspondantes de G_1, respectivement G_2. Alors $e_{G_1\times G_2} := (e_{G_1}, e_{G_2})$, $(x_1,x_2)^{-1} := (x_1^{-1}, x_2^{-1})$ et l'associativité est évidente car

$$((x_1,x_2)(y_1,y_2))(z_1,z_2) = ((x_1y_1, x_2y_2))(z_1,z_2) = ((x_1y_1)z_1, (x_2y_2)z_2) =$$
$$= (x_1(y_1z_1), x_2(y_2z_2)) = (x_1,x_2)(y_1z_1, y_2z_2) = (x_1,x_2)((y_1,y_2)(z_1,z_2)).$$

En effet l'associativité composante par composante donne l'associativité de la loi des couples.

Donnons la table de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(\bar 0,\bar 0), (\bar 0,\bar 1), (\bar 1,\bar 0), (\bar 1,\bar 1)\}$ pour la loi + de ce groupe produit.

$+$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 1)$	$(\bar 1,\bar 0)$	$(\bar 1,\bar 1)$
$(\bar 0,\bar 0)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 1)$	$(\bar 1,\bar 0)$	$(\bar 1,\bar 1)$
$(\bar 0,\bar 1)$	$(\bar 0,\bar 1)$	$(\bar 0,\bar 0)$	$(\bar 1,\bar 1)$	$(\bar 1,\bar 0)$
$(\bar 1,\bar 0)$	$(\bar 1,\bar 0)$	$(\bar 1,\bar 1)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 1)$
$(\bar 1,\bar 1)$	$(\bar 1,\bar 1)$	$(\bar 1,\bar 0)$	$(\bar 0,\bar 1)$	$(\bar 0,\bar 0)$

Pour $e = (\bar 0,\bar 0)$, $x = (\bar 0,\bar 1)$, $y = (\bar 1,\bar 0)$, $z = (\bar 1,\bar 1)$ c'est la table G_1. Donc $(G_1,\cdot)$ est un groupe de même structure que $((\mathbb{Z}/2\mathbb{Z})^2,+)$ (autre notation de $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$)

Par conséquent il existe deux structures de groupe possibles sur un ensemble à 4 éléments. De toute évidence ces structures sont distinctes car si on regarde les ordres des éléments on s'aperçoit que dans $\mathbb{Z}/4\mathbb{Z}$, $\mathrm{ord}(\bar 1) = 4$, $\mathrm{ord}(\bar 2) = 2$, $\mathrm{ord}(\bar 3) = 4$ (car $\bar 1 + \bar 1 = \bar 2 \neq \bar 0$, $\bar 1+\bar 1+\bar 1 = \bar 3 \neq \bar 0$ et il faut additionner $\bar 1$ quatre fois pour aboutir à $\bar 0$). De même $\bar 3 + \bar 3 = \bar 2 \neq \bar 0$, $\bar 3+\bar 3+\bar 3 = \bar 1 \neq \bar 0$ et il faut additionner $\bar 3$ quatre fois pour aboutir à $\bar 0$. Or dans $(\mathbb{Z}/2\mathbb{Z})^2$ on a $\mathrm{ord}(\bar 0,\bar 1) = \mathrm{ord}(\bar 1,\bar 0) = \mathrm{ord}(\bar 1,\bar 1) = 2$ donc il n'y a pas d'élément d'ordre 4 dans $(\mathbb{Z}/2\mathbb{Z})^2$. Dans une structure identique les ordres des éléments doivent être identiques, ce n'est pas le cas ici.

ex5 Soit $x, y \in G$. On a $(xy)^2 = xyxy = 1$ donc

$x(xyxy)y = x.1.y = xy$ Or $x^2 = y^2 = 1$ donc

$x^2yxy^2 = yx = xy$. Ceci montre que G est abélien (càd commutatif).

ex6 On a $yx = xyy = yx^2y$ donc $y^{-1}yx = y^{-1}yx^2y$

donc $x = x^2y$ d'où $x^{-1}x = x^{-1}xxy$ càd $1 = xy$.

Donc $yx = xyy = 1.y = y$ d'où $y^{-1}yx = y^{-1}y = x = 1$.

Alors de $xy = 1$ on tire $1 = 1.y = y$. Finalement $x = y = 1$.

ex7 On donne d'abord une condition nécessaire et suffisante pour qu'une partie H d'un groupe G soit un sous-groupe de G : (notation $H < G$).

$\boxed{\text{Lemme clé}}$ Si $H \subset G$ avec $(G, \cdot)$ groupe et $H \neq \emptyset$ alors $(H, \cdot)$ est un sous-groupe de G ssi $\forall x, y \in H$, $xy^{-1} \in H$

<u>Preuve</u> "$\Rightarrow$" L'implication directe est facile car si $(H, \cdot)$ est un sous-groupe de G alors $\forall x, y \in H$ on a $y^{-1} \in H$ et $x.y^{-1} \in H$. En effet $(H, \cdot)$ est un groupe et donc chaque élément de H admet un inverse dans H et la loi $\cdot$ est interne dans H.

"$\Leftarrow$" L'implication réciproque se démontre en étapes. Comme $H \neq \emptyset$ on prend $x \in H$ et $y = x \in H$. Alors $xy^{-1} = xx^{-1} = e \in H$ par la propriété de H d'être stable pour les produits xy^{-1} lorsque x, y sont dans H.

Maintenant si on prend $x = e$ et $y \in H$ on sait que $ey^{-1} = y^{-1} \in H$ donc H est stable par passage à l'inverse.

Si on prend alors $x, y \in H$, comme $y^{-1} \in H$, on a $x(y^{-1})^{-1} \in H$. Or $(y^{-1})^{-1} = y$ donc $xy \in H$ et la loi $\cdot$ est interne dans H.

Finalement cette loi était associative dans G donc elle reste associative dans H et H est bien un sous-groupe de G.

Cela finit la preuve du lemme, bien utile pour remplacer toutes les vérifications nécessaires pour établir que $H \subset G$, $H \neq \emptyset$ est un sous-groupe de G par une unique condition.

ex7 q1) Si $z_1, z_2 \in U_n$ on a $(z_1 z_2^{-1})^n = z_1^n z_2^{-n} = \frac{z_1^n}{z_2^n} = 1$ donc $z_1 z_2^{-1} \in U_n$ et $(U_n, \times)$ est bien un sous-groupe de $(\mathbb{C}^*, \times)$ d'après le lemme clé.

q2) Soit $\omega = e^{\frac{2\pi i}{n}}$ et $z \in U_n$. On a $z^n = 1$ donc $|z|^n = 1$ d'où $|z| = 1$ car $|z| \in \mathbb{R}_+$. Alors $z = e^{i\theta}$ avec $\theta \in [0, 2\pi[$ et $z^n = e^{ni\theta} = 1 = e^{2\pi i k}$ avec $k \in \mathbb{Z}$. On a $n\theta = 2\pi k$ donc $\theta = \frac{2\pi k}{n}$ et pour que $\theta \in [0, 2\pi[$ on doit prendre $k \in \{0, \dots, n-1\}$.
Par conséquent $z = e^{i\frac{2\pi k}{n}} = \omega^k$ donc ω engendre U_n et U_n a au plus n éléments : $\omega^0 = 1, \omega, \omega^2, \dots, \omega^{n-1}$. Vérifions que tous ces éléments sont distincts. En effet si $\omega^{k_1} = \omega^{k_2}$ avec $k_1, k_2 \in \{0, \dots, n-1\}$ on a $\omega^{k_1 - k_2} = 1$. Donc $\frac{(k_1 - k_2) 2\pi}{n} = 2\pi l$ avec $l \in \mathbb{Z}$ d'où $k_1 - k_2 = nl$ avec $l \in \mathbb{Z}$. Mais $\left.\begin{array}{l} 0 \leq k_1 \leq n-1 \\ 1-n \leq -k_2 \leq 0 \end{array}\right\} \Rightarrow 1-n \leq k_1 - k_2 \leq n-1$

donc $|k_1 - k_2| \leq n-1$ d'où $|nl| = n|l| \leq n-1$ c'à'd $|l| < 1$, $l \in \mathbb{Z}$ c'à'd $l = 0$. Finalement $k_1 - k_2 = 0$ donc $k_1 = k_2$. Alors pour $i \neq j$ on aura $\omega^i \neq \omega^j$ lorsque $i, j \in \{0, \dots, n-1\}$ et U_n est formé par exactement n éléments de la forme ω^k, $k \in \{0, \dots, n-1\}$.
On a bien $U_n = \{1, \omega, \dots, \omega^{n-1}\}$ donc U_n cyclique d'ordre n.

q3) "$\Rightarrow$" Si $m | n$ on a $n = mk$ donc pour $z \in U_m$ on a $z^n = z^{mk} = (z^m)^k = 1$ donc $z \in U_n$. On a bien $U_m \subset U_n$ et même $U_m < U_n$ (c'à'd U_m sous-groupe de U_n) car si $z_1, z_2 \in U_m$, on a $(z_1 z_2^{-1})^m = z_1^m z_2^{-m} = \frac{z_1^m}{z_2^m} = 1$ donc $z_1 z_2^{-1} \in U_m$.
"$\Leftarrow$" Si $U_m \subset U_n$ on a en fait $U_m < U_n$ comme ci-dessus donc d'après le théorème de Lagrange l'ordre de U_m (qui est m) divise l'ordre de U_n (qui est n, d'après la q2).

<u>Remarque</u> On aurait pu résoudre la q2) en montrant que le groupe $(\mathcal{U}_n, \cdot)$ est isomorphe au groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$.

Pour cela on peut définir une application $f : (\mathbb{Z}/n\mathbb{Z}, +) \longrightarrow (\mathcal{U}_n, \cdot)$
$\bar{k} \longmapsto e^{\frac{2\pi i k}{n}}$

On montre d'abord que f est <u>bien défini</u> càd que
$f(\bar{k}) = f(\overline{k+\ell n})$ pour $\ell \in \mathbb{N}$ (cela signifie que la définition de f ne dépend pas du représentant k choisi dans la classe $\bar{k} = \{k+n\ell \mid \ell \in \mathbb{Z}\}$).

En effet $e^{\frac{2\pi i(k+\ell n)}{n}} = e^{\frac{2\pi i k}{n}} e^{\frac{2\pi i \ell n}{n}} = e^{\frac{2\pi i k}{n}} e^{2\pi i \ell} = e^{\frac{2\pi i k}{n}}$
car $e^{2\pi i \ell} = 1$.

On montre ensuite que f est un <u>morphisme</u> càd que
$f(\bar{k}_1 + \bar{k}_2) = f(\bar{k}_1) f(\bar{k}_2)$, or $f(\bar{k}_1 + \bar{k}_2) = f(\overline{k_1+k_2}) = e^{\frac{2\pi i(k_1+k_2)}{n}}$
$= e^{\frac{2\pi i k_1}{n}} e^{\frac{2\pi i k_2}{n}} = f(\bar{k}_1) f(\bar{k}_2)$.

Puisqu'il s'agit d'un morphisme, on peut caractériser son injectivité à partir du noyau de f (c'est toujours dans cet ordre qu'il faut s'y prendre car avant de savoir que f était un morphisme on ne pouvait pas parler de noyau pour f)

Or $\operatorname{Ker} f = \{\bar{k} \mid f(\bar{k}) = 1\} = \{\bar{k} \mid e^{\frac{2\pi i k}{n}} = 1\} = \{\bar{k} \mid \frac{k}{n} \in \mathbb{Z}\} = \{\bar{k} \mid k = n\ell,\ \ell \in \mathbb{Z}\}$
$= \{\bar{0}\}$ donc f est en effet une application injective.

On peut montrer directement que $|\mathcal{U}_n| = n$ en remarquant que les éléments de $\mathcal{U}_n$ sont les n racines dans $\mathbb{C}$ du polynôme $x^n - 1$ qui n'a pas de racine multiple puisque $(x^n-1)' = nx^{n-1}$ donc il n'y a pas de zéro commun de $g(x) = x^n - 1$ et $g'(x) = nx^{n-1}$. Alors f est bijective en raison de l'égalité des cardinaux finis de $\mathbb{Z}/n\mathbb{Z}$ et $\mathcal{U}_n$ $(n \geq 1)$.

Sinon la surjectivité de f se prouve en posant pour $z \in \mathbb{C}$ tq $z^n = 1$ que $z = e^{i\theta}$ (car $|z| = 1$) vérifie $e^{i\theta n} = 1$ donc $\theta n = 2\pi \ell$ pour $\ell \in \mathbb{Z}$ d'où $\theta = \frac{2\pi \ell}{n}$ et $f(\bar{\ell}) = z$ lorsque $z = e^{\frac{2\pi i \ell}{n}}$. La cyclicité de $\mathcal{U}_n$ découle de celle de $\mathbb{Z}/n\mathbb{Z}$ et par exemple $\mathcal{U}_n = \langle e^{\frac{2\pi i}{n}} \rangle = \langle f(\bar{1}) \rangle = \langle f(\bar{k}) \rangle$ tq $k \wedge n = 1$.

ex8 On montre d'abord les lemmes suivants : Soit G un groupe et $x \in G$, $n \in \mathbb{N}^*$

Lemme 1 : Si $\mathrm{ord}(x) = n$ et $x^{\ell} = 1$ alors $n \mid \ell$.

Preuve lemme 1 Ecrivons la division euclidienne de ℓ par n :

$\ell = nq + r$, $0 \leq r < n$. Alors $x^{\ell} = (x^n)^q x^r = 1^q x^r = x^r = 1$

Or d'après la définition de l'ordre de x on a pour $n \geq 1$, $n \in \mathbb{N}$

($\mathrm{ord}(x) = n$ ssi $x^n = 1$ et $\forall m \in \mathbb{N}^*$, $m < n$, $x^m \neq 1$)

Donc si $x^r = 1$ avec $r < n$ c'est que $r = 0$ et donc que $n \mid \ell$ ■

Lemme 2 Si $\mathrm{ord}(x) = n$ et $k \in \mathbb{Z}$ alors $\mathrm{ord}(x^k) = \frac{n}{n \wedge k}$

(rappel de notation : $n \wedge k := \mathrm{pgcd}(n, k)$)

Preuve lemme 2 Notons $d = n \wedge k$ et regardons $(x^k)^{\frac{n}{d}} = (x^n)^{\frac{k}{d}}$

(ceci est possible car $d \mid k$ donc $\frac{k}{d} \in \mathbb{Z}$). Comme $x^n = 1$ on a

bien $(x^k)^{\frac{n}{d}} = 1^{\frac{k}{d}} = 1$.

Prenons $\ell \in \mathbb{N}^*$ tq $(x^k)^{\ell} = 1$. On a $x^{k\ell} = 1$ donc d'après le lemme 1

on a $n \mid k\ell$. On ne peut pas appliquer le lemme de Gauss car nous ne savons pas si $n \wedge k = 1$. On peut cependant affirmer que

$\frac{n}{d} \,\Big|\, \frac{k}{d} \cdot \ell$ et appliquer maintenant le lemme de Gauss, vu que

$\mathrm{pgcd}\left(\frac{n}{d}, \frac{k}{d}\right) = 1$. Par conséquent $\frac{n}{d} \,\Big|\, \ell$ donc $\frac{n}{d} \leq \ell$. Cela montre

que $\frac{n}{d}$ est la plus petite puissance strictement positive de x^k

telle que x^k élevé à cette puissance donne 1. Donc que $\mathrm{ord}(x^k) = \frac{n}{d}$ ■

On peut se servir de ces résultats pour déduire rapidement

les ordres des éléments des groupes cycliques, comme $\mathbb{Z}/n\mathbb{Z}$, car

vu que $\mathrm{ord}(\bar{1}) = n$, on a alors d'après le lemme 2 que

$\mathrm{ord}(\bar{k}) = \frac{n}{n \wedge k}$.

On écrit les ordres des éléments demandés sous forme de tableaux :

$\mathbb{Z}/12\mathbb{Z}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}=\overline{-5}$	$\bar{8}=\overline{-4}$	$\bar{9}=\overline{-3}$	$\overline{10}=\overline{-2}$	$\overline{11}=\overline{-1}$
ordre	1	12	6	4	3	12	2	12	3	4	6	12

les calculs des ordres étant faits en utilisant la formule $\mathrm{ord}(\bar{k}) = \dfrac{12}{k \wedge 12}$.

On a bien sûr ($\mathrm{ord}(\bar{k}) = 12$ ssi $k \wedge 12 = 1$) donc les générateurs de $\mathbb{Z}/12\mathbb{Z}$ sont exactement ses éléments inversibles pour la multiplication.

Par conséquent $(\mathbb{Z}/12\mathbb{Z})^* = \{\bar{k} \in \mathbb{Z}/12\mathbb{Z} \mid \exists\, \bar{l} \in \mathbb{Z}/12\mathbb{Z} \text{ tq } \bar{k}\bar{l} = \bar{1}\} =$

$= \{\bar{1}, \bar{5}, \bar{7}, \overline{11}\}$ qui est bien de cardinal $\varphi(12) = \varphi(2^2 \cdot 3) =$

$= \varphi(2^2)\varphi(3) = (2^2 - 2)(3-1) = 4$.

On a $\mathrm{ord}(\bar{1}) = 1$ vu que $\bar{1}$ est l'élément neutre de $(\mathbb{Z}/12\mathbb{Z})^*$,

on a $\bar{5}^2 = \overline{25} = \bar{1}$ donc $\mathrm{ord}(\bar{5}) = 2$ dans ce contexte.

On a aussi $\bar{7}^2 = \overline{-5}^2 = \overline{49} = \overline{25} = \bar{1}$ donc $\mathrm{ord}(\bar{7}) = \mathrm{ord}(\overline{-5}) = 2$

et $\overline{11}^2 = \overline{-1}^2 = \overline{121} = \bar{1}$ donc $\mathrm{ord}(\overline{11}) = \mathrm{ord}(\overline{-1}) = 2$.

Sous forme de tableau cela donne

$\mathbb{Z}/12\mathbb{Z}^*$	$\bar{1}$	$\bar{5}$	$\bar{7}=\overline{-5}$	$\overline{11}=\overline{-1}$
ordre	1	2	2	2

Donc $((\mathbb{Z}/12\mathbb{Z})^*, \cdot)$ n'est pas un groupe cyclique (il ne contient pas d'élément d'ordre 4). D'après les tables trouvées à l'exercice 4 il s'agit d'un groupe isomorphe à $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$.

<u>Remarque</u> Pour simplifier les calculs si n est grand on peut astucieusement remplacer les classes $\overline{n-k}$ par $\overline{-k}$ pour $k < \frac{n}{2}$, vu que $(-k) \wedge n = k \wedge n$. Cela permet par exemple de donner rapidement

$\mathbb{Z}/20\mathbb{Z}$	$\bar{0}$	$\overline{\pm 1}$	$\overline{\pm 2}$	$\overline{\pm 3}$	$\overline{\pm 4}$	$\overline{\pm 5}$	$\overline{\pm 6}$	$\overline{\pm 7}$	$\overline{\pm 8}$	$\overline{\pm 9}$	$\overline{10}$
ordre	1	20	10	20	5	4	10	20	5	20	2

et ensuite

$(\mathbb{Z}/20\mathbb{Z})^*$	$\bar{1}$	$\overline{-1}$	$\overline{\pm 3}$	$\overline{\pm 7}$	$\overline{\pm 9}$
ordre	1	2	4	4	2

car $|\mathbb{Z}/20\mathbb{Z}^*| = 8$ et d'après le théorème de Lagrange les ordres des éléments $\neq \bar{1}$ sont des diviseurs de 8, donc pairs.

ex.9 On a $H \subset G$ et $H \neq \emptyset$ car $1 \in H$ $(\mathrm{ord}(1)=1)$.

On veut montrer que si $\mathrm{ord}(x)$ et $\mathrm{ord}(y)$ sont finis alors $\mathrm{ord}(xy^{-1})$ est fini.

Mais si $\mathrm{ord}(x)=n$ et $\mathrm{ord}(y)=m$, alors $(xy^{-1})^{nm} = (x^n)^m (y^m)^{-n} = 1$

puisque le groupe G est abélien. Donc $\mathrm{ord}(xy^{-1}) \leq nm$ et il est par conséquent fini. D'après le lemme clé, H est bien un sous groupe de G.

ex.10 On a que $H = \{ e^{2\pi i r} \mid r \in \mathbb{Q} \}$ est un sous-groupe de $(\mathbb{C}^*, \cdot)$ car

$0 \notin H$, $H \neq \emptyset$ et $e^{2\pi i r_1} (e^{2\pi i r_2})^{-1} = e^{2\pi i (r_1 - r_2)} \in H$

vu que $r_1, r_2 \in \mathbb{Q}$ donc que $r_1 - r_2 \in \mathbb{Q}$.

Ce groupe est infini puisque pour $r_n = \frac{1}{n}$, $n \in \mathbb{N}^*$ on a $u_n = e^{2\pi i r_n} \in H$

et $u_k \neq u_l$ $\forall k \neq l$. En effet, si $u_k = u_l$ on a $e^{\frac{2\pi i}{k}} = e^{\frac{2\pi i}{l}}$

donc $\frac{2\pi}{k} = \frac{2\pi}{l} + 2\pi s$ avec $s \in \mathbb{Z}$. Donc $s = \frac{1}{k} - \frac{1}{l} = \frac{l-k}{kl}$

et comme $\begin{cases} 0 < \frac{1}{k} \leq 1 \\ -1 \leq -\frac{1}{l} < 0 \end{cases}$ on a $-1 < \frac{1}{k} - \frac{1}{l} < 1$ donc

$-1 < s < 1$ avec $s \in \mathbb{Z}$ c'à'd $s = 0$. Donc $k = l$.

Cela prouve l'existence d'une suite infinie d'éléments distincts de H

donc $|H| = +\infty$. Mais si $r = \frac{p}{q}$ avec $p \wedge q = 1$, $p, q \in \mathbb{Z}$, $p \neq 0$, $q > 0$

alors $\mathrm{ord}(e^{2\pi i \frac{p}{q}}) = q$ car $(e^{2\pi i \frac{p}{q}})^q = 1$ et si $(e^{2\pi i \frac{p}{q}})^l = 1$, $l \in \mathbb{N}^*$

on a $\frac{2\pi i p l}{q} = 2\pi i t$ avec $t \in \mathbb{Z}$ donc $pl = qt$. Comme $q \mid pl$

et que $q \wedge p = 1$ d'après le lemme de Gauss on a que $q \mid l$ donc $q \leq l$.

Par conséquent H est un groupe infini dans lequel tout élément est d'ordre fini.

Ex 11 Les éléments $g \in G \setminus \{1\}$ sont tels que $\mathrm{ord}(g) \mid 35$ d'après le théorème de Lagrange. Donc $\mathrm{ord}(g) \in \{5, 7, 35\}$. S'il existe $g \in G$ tel que $\mathrm{ord}(g) = 35$ alors $\mathrm{ord}(g^7) = \frac{35}{\mathrm{pgcd}(35,7)} = \frac{35}{7} = 5$ et

$$\mathrm{ord}(g^5) = \frac{35}{\mathrm{pgcd}(35,5)} = \frac{35}{5} = 7.$$

Si aucun élément de G n'est d'ordre 35, il y a alors des éléments d'ordre 5 ou d'ordre 7.

Supposons par l'absurde que tous les éléments $g \in G \setminus \{1\}$ sont d'ordre 5. Alors chaque tel g engendre un sous-groupe H_g de cardinal 5 et si $g \neq g'$ on a $H_g \cap H_{g'} = \begin{cases} \{1\} \\ H_g \end{cases}$ ou (en effet $H_g \cap H_{g'} = H$ est un sous-groupe de H_g et de $H_{g'}$, donc de cardinal 1 ou 5. Si $|H| = 1$ alors $H = \{1\}$, sinon $H = H_g = H_{g'}$). Comme $G = \bigcup_{g \in G} H_g$ et que tous les sous-groupes H_g distincts ne se coupent que en $\{1\}$ on a que $35 = 1 + 4n$ avec n le nombre de sous-groupes H_g distincts. Or $4 \nmid 34$ donc cette situation est impossible.

Supposons par l'absurde que tous les éléments $g \in G \setminus \{1\}$ sont d'ordre 7. Alors on reprend le raisonnement ci-dessus avec les sous-groupes H_g de cardinal 7 engendrés par de tels g. On aura de nouveau $H = H_g \cap H_{g'} = \{1\}$ ou H_g car $|H| = 1$ ou 7. Alors $35 = 1 + 6m$ avec m le nombre de sous-groupes H_g distincts. Or $6 \nmid 34$ donc cette situation est également impossible.

La seule possibilité est alors qu'il existe au moins un élément d'ordre 5 et un élément d'ordre 7.

ex 12 q1) On a $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in Sl_2(\mathbb{Z})$ et la multiplication des matrices est associative d'élément neutre I_2.

De plus $\det(AB) = \det(A)\det(B) = 1$ si $A, B \in Sl_2(\mathbb{Z})$ donc $AB \in Sl_2(\mathbb{Z})$, les coefficients de AB étant encore entiers.

Par conséquent $Sl_2(\mathbb{Z})$ est stable pour la multiplication.

Lorsque $\det(A) = 1$ on a $A^{-1} = {}^t\mathrm{com}(A) \in Sl_2(\mathbb{Z})$, où ${}^t\mathrm{com}(A)$ est la transposée de la comatrice de A (en général pour une matrice inversible $A^{-1} = \frac{1}{\det A}\, {}^t\mathrm{com}(A)$). Donc $Sl_2(\mathbb{Z})$ est stable aussi par inverse. En conclusion $Sl_2(\mathbb{Z})$ est un groupe multiplicatif.

Il est clairement infini car $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \in Sl_2(\mathbb{Z})$, $\forall k \in \mathbb{Z}$.

Il n'est pas commutatif car en prenant par exemple $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ comme à la question 2, on a $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $BA = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \neq AB$.

q2) On calcule $A^2 = -I_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ donc $A^3 = -A$ et $A^4 = I_2$ donc $\mathrm{ord}(A) = 4$.

On a $B^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$, $B^3 = I_2$ donc $\mathrm{ord}(B) = 3$. On remarque ensuite que $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ pour $n \in \mathbb{N}^*$. Cette propriété se démontre par récurrence : c'est évident pour $n = 1$ et si elle est vraie au rang n on a $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{n+1} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$ donc elle est vraie aussi au rang $n+1$. Par conséquent $AB^n = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n \neq I_2$ $\forall n \in \mathbb{N}^*$ donc $\mathrm{ord}(AB) = +\infty$.

Cette situation peut servir de contre-exemple à l'exercice 9 ; dans un cadre non-commutatif l'ensemble $H = \{x \in G \mid \mathrm{ord}(x) \text{ fini}\}$ peut ne pas être stable pour la multiplication, donc ne pas être un sous-groupe. De même à l'exercice 13, si les éléments x et y considérés ne commutent pas (comme $x = A$, $y = B$ ici), même si $\mathrm{ord}(x) \wedge \mathrm{ord}(y) = 1$ (c'est le cas ici, vu que $\mathrm{ord}(A) = 4$ et $\mathrm{ord}(B) = 3$), on n'a pas $\mathrm{ord}(xy) = \mathrm{ord}(x)\,\mathrm{ord}(y)$ (car $\mathrm{ord}(AB) = +\infty$)

ex 13 On a $(xy)^{ab} = x^{ab} y^{ab}$ puisque les éléments x et y commutent donc $xy = yx$ et $\underbrace{xyxy\cdots xy}_{ab \text{ fois}} = x^{ab} y^{ab}$.

Or $x^a = 1$ et $y^b = 1$ donc $(xy)^{ab} = (x^a)^b (y^b)^a = 1$.

On a aussi que si $l \in \mathbb{N}^*$ et $(xy)^l = 1$ alors $x^l y^l = 1$ donc $x^l = y^{-l}$. Par conséquent $x^{la} = y^{-la} = (x^a)^l = 1$.

On en déduit, vu que $b = \text{ord}(y)$, que $b \mid -la$. Or $\text{pgcd}(a, b) = 1$ donc d'après le lemme de Gauss on a que $b \mid l$.

On écrit également $x^{lb} = y^{-lb} = 1$ et on en déduit que $a \mid lb$ (vu que $\text{ord}(x) = a$) et encore, puisque $\text{pgcd}(a,b) = 1$, que $a \mid l$ par le lemme de Gauss. Vu de nouveau que $\text{pgcd}(a, b) = 1$, des divisibilités ci-dessus on peut conclure que $ab \mid l$ donc que $\text{ord}(xy) = ab$, car plus petit exposant l tel que $(xy)^l = 1$.

⚠ Sans que toutes les hypothèses de cet exercice soient vérifiées on ne peut pas obtenir l'ordre de xy en général !

Par exemple si $xy = yx$ mais $\text{pgcd}(a,b) \neq 1$ on n'aura pas toujours $\text{ord}(xy) = ab$ ni même $\text{ord}(xy) = \text{ppcm}(a,b)$ comme le montre le cas de $y = x^{-1}$ avec $x \neq 1$ (donc $\text{ord}(x) = \text{ord}(y) = a > 1$). Dans ce cas $xy = yx = 1$ et $\text{ord}(1) = 1 \neq a^2$ et $\text{ord}(1) \neq a$ aussi ($a = \text{ppcm}(a,a)$).

De même si $xy \neq yx$ on peut avoir $x = (12)$, $y = (123) \in S_3$ (le groupe symétrique) avec $\text{ord}(x) = a = 2$, $\text{ord}(y) = b = 3$, $\text{pgcd}(a,b) = 1$ mais $xy = (23)$, $\text{ord}(xy) = 2$, et $yx = (13)$, $\text{ord}(yx) = 2$. Il n'y a pas dans S_3 des éléments d'ordre $6 = 2 \cdot 3 = \text{ppcm}(2,3)$. Voir aussi la remarque à la fin de l'exercice 12.

ex 14

On a $\mathbb{Z}/13\mathbb{Z}^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \overline{10}, \overline{11}, \overline{12}\}$

groupe pour la multiplication, d'élément neutre $\bar{1}$.

On a $\bar{2}^2 = \bar{4}$, $\bar{2}^3 = -\bar{5}$, $\bar{2}^4 = \bar{3}$, $\bar{2}^5 = \bar{6}$, $\bar{2}^6 = -1$ donc
($\bar{2}^7 = -\bar{2}$, $\bar{2}^8 = -\bar{4}$, $\bar{2}^9 = \bar{5}$, $\bar{2}^{10} = -\bar{3}$, $\bar{2}^{11} = -\bar{6}$, $\bar{2}^{12} = \bar{1}$)
$\mathrm{ord}(\bar{2}) = 12$ et $\bar{2}$ engendre bien $(\mathbb{Z}/13\mathbb{Z})^*$ qui est de cardinal 12.

On peut faire un tableau plus complet avec les ordres de tous les éléments de $(\mathbb{Z}/13\mathbb{Z})^*$

$(\mathbb{Z}/13\mathbb{Z})^*$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}=-\bar{6}$	$\bar{8}=-\bar{5}$	$\bar{9}=-\bar{4}$	$\overline{10}=-\bar{3}$	$\overline{11}=-\bar{2}$	$\overline{12}=-\bar{1}$
ordre	1	12	3	6	4	12	12	4	3	6	12	2

On s'est servi de la formule $\mathrm{ord}(x^k) = \dfrac{\mathrm{ord}(x)}{k \wedge \mathrm{ord}(x)}$ en remarquant que

$\bar{3} = \bar{2}^4$ donc $\mathrm{ord}(\bar{3}) = \dfrac{12}{4 \wedge 12} = 3$, $\bar{4} = \bar{2}^2$ donc $\mathrm{ord}(\bar{4}) = \dfrac{12}{2 \wedge 12} = 6$

$\bar{5} = \bar{2}^9$ donc $\mathrm{ord}(\bar{5}) = \dfrac{12}{9 \wedge 12} = 4$, $\bar{6} = \bar{2}^5$ donc $\mathrm{ord}(\bar{6}) = \dfrac{12}{5 \wedge 12} = 12$.

$\bar{7} = -\bar{6} = \bar{2}^{11}$ donc $\mathrm{ord}(\bar{7}) = \dfrac{12}{11 \wedge 12} = 12$, $\bar{8} = -\bar{5} = \bar{2}^3$ donc $\mathrm{ord}(\bar{8}) = \dfrac{12}{3 \wedge 12} = 4$

$\bar{9} = -\bar{4} = \bar{2}^8$ donc $\mathrm{ord}(\bar{9}) = \dfrac{12}{8 \wedge 12} = 3$, $\overline{10} = -\bar{3} = \bar{2}^{10}$ donc $\mathrm{ord}(\overline{10}) = \dfrac{12}{10 \wedge 12} = 6$

$\overline{11} = -\bar{2} = \bar{2}^7$ donc $\mathrm{ord}(\overline{11}) = \dfrac{12}{7 \wedge 12} = 12$, $\overline{12} = -\bar{1} = \bar{2}^6$ donc $\mathrm{ord}(\overline{12}) = \dfrac{12}{6 \wedge 12} = 2$

On voit que, comme dans tout groupe cyclique de cardinal 12, il y a $\varphi(12) = 4$ générateurs ($\bar{2}$, $\bar{6}$, $-\bar{6}$ et $-\bar{2}$), il y a $\varphi(6) = 2$ éléments d'ordre 6 ($\bar{4}$ et $-\bar{3}$), il y a $\varphi(4) = 2$ éléments d'ordre 4 ($\bar{5}$ et $-\bar{5}$), il y a $\varphi(3) = 2$ éléments d'ordre 3 ($\bar{3}$ et $-\bar{4}$) et il y a $\varphi(2) = 1$ élément d'ordre 2 ($-\bar{1}$).